NAVY MEDICINE
World Class Care…Anytime, Anywhere

Medical Devices on the Network

Presented by:
CDR James Martin
&
CDR Richard Makarski

Learning Objectives

- Understand the background and history of the Medical Device STIG
  - STIG does not provide a get-out-of-jail card for compliancy
  - Medical Device STIG is a living document; feedback is currently being solicited for the first update
- Understand what a medical device is
- Understand the possible security options for security non-compliant medical devices on a network

Agenda

- Medical Device STIG Background
- STIG Purpose
- Definition of Medical Device
- Device Compliancy
- Device Separation
  - VLAN Separation
  - Security Zone
  - Screened Subnet
- STIG Current Status
- Proposed Revisions

Medical Device STIG Background

- Created based on the need to mitigate risks to the DoD/Service Networks and to the medical devices
  - The risks revolve around the inability of MHS IA workforce members to adequately and efficiently patch known vulnerabilities – often having to rely on the medical device vendor
- Provides guidance on establishing acceptable alternatives to protect Network security in those cases where full compliance with DoD/DoN policy cannot be achieved in a timely manner

Medical Device STIG Timeline

- Late 2008 – Navy Medicine personnel authored a draft and began work with Army, Air Force, and DISA to validate/update draft
- Late 2009 – Concluded validation/update process and submitted to DISA for processing
- Early 2010 – TIM held comprising members of the Navy (including NETWARCOM), Army, Air Force, DISA, and TMA
- JUN 2010 – Navy presented the revised STIG to the DSAWG where it was approved unanimously
- 27 JUL 2010 – STIG signed
- Today – Initial call for updates to STIG

Purpose of the Medical Device STIG

- Provides guidance to implement secure IS and networks
  - Ensures that medical devices continue to provide healthcare without risking safety to the patient
- Condenses multiple sources of information into one document
- Provides support for senior policy makers by laying out the need to balance patient care and the protection of the network
- Designed to call out the unique problems faced by the medical community when vendors may be slow or resistant to updating products to DoD standards

Medical Device Defined

- A medical device is a device that has been approved by the FDA
- 3 categories of medical devices (Types I, II, III)
  - Ranges from those that have no active role in patient care (Type-I) to those that directly monitor or sustain patient health (Type-II)
- Critical systems (Type-III) are most likely to be impacted when forced into a compliancy state when the device or vendor has not had the chance to evaluate the patch or update mandated by DoD

Compliancy

- The Medical Device STIG does not provide get-out-of-jail card with regard to compliancy requirements
  - STIG does acknowledge that compliancy cannot always be achieved within the timeframe required by DoD/DoN
- All cases where compliancy (STIG, IAVM, etc.) cannot be achieved, or cannot be achieved within Agency/Service established timeframes:
  1. The vendor should be notified
  2. POA&M should be generated and submitted to the DAA for approval

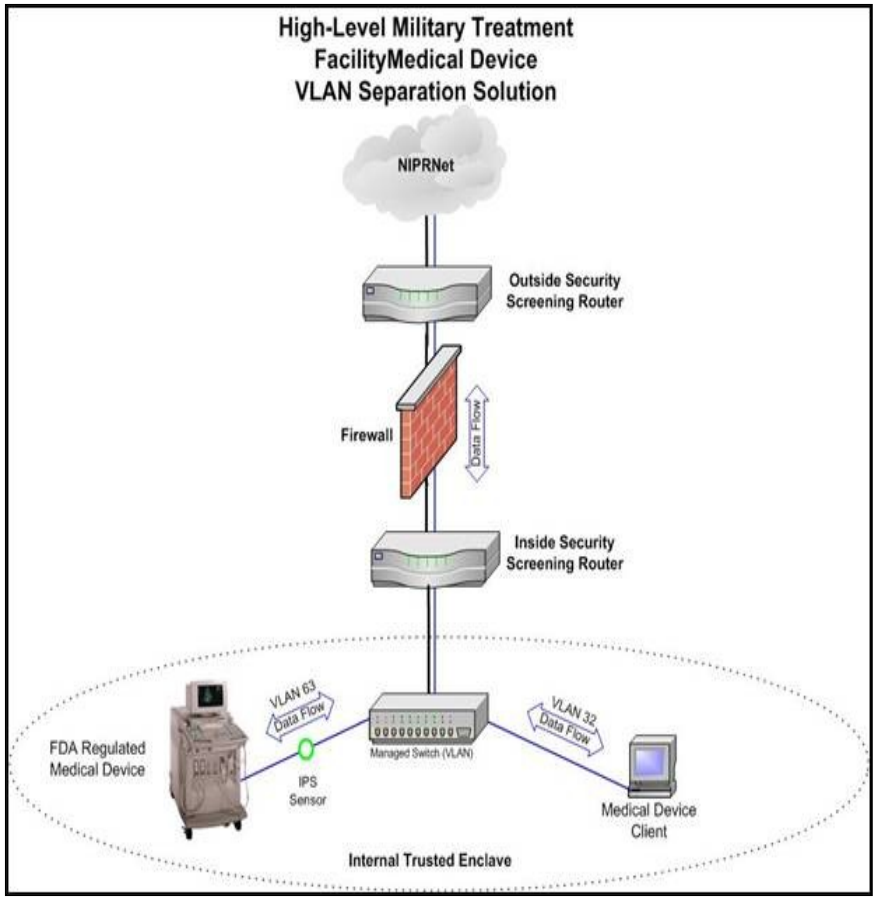
Compliancy or Separation

- A medical device that is compliant with all DoD/DoN policy directives can be placed on the network the same as any other IA device
- A medical device that cannot be made compliant, or cannot be made compliant within guidelines established by DoD/DoN, must be separated from the site network
- 3 approved separation options are identified in the Medical Device STIG:
  - VLAN Separation, Security Zone, Screened Subnet

VLAN Separation

VLAN Separation Solution

- Medical devices and their associated systems are grouped together in a separate network segment to form a broadcast domain
- Provides layer of security by incorporating implicit access control lists on the OSSR, ISSR, IPS, and managed switches
- Isolates the devices from the rest of the network, but it does not solve IAVM compliance issues

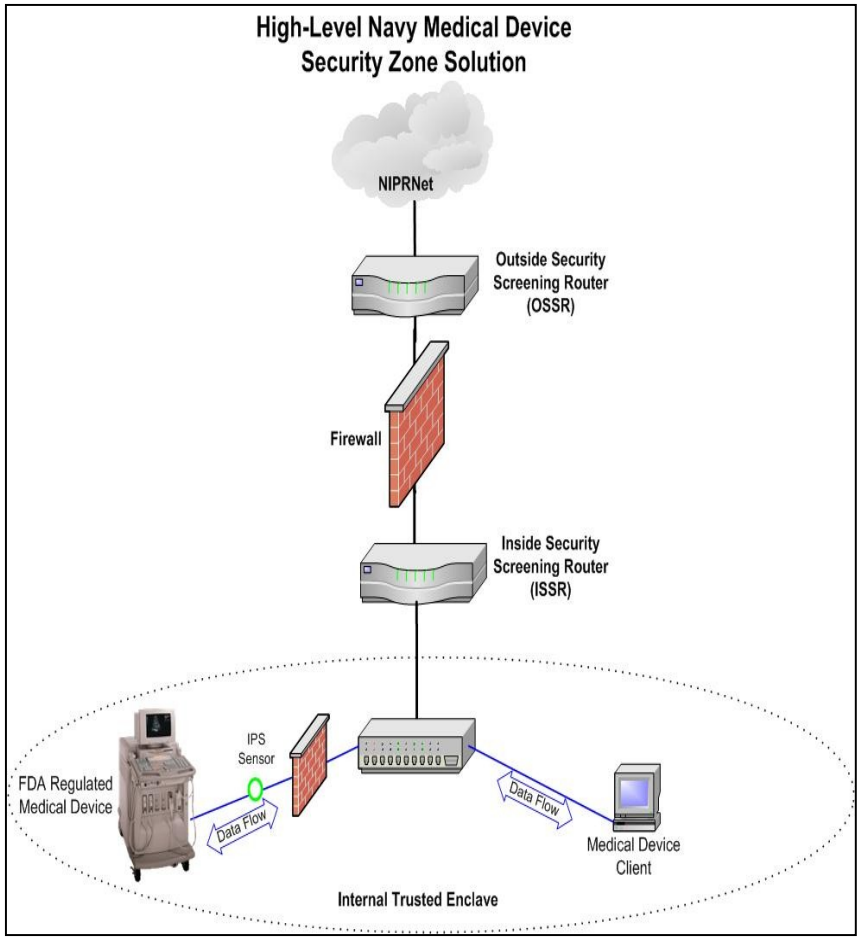


Used within trusted network or when using compliant ports across boundaries

Security Zone

Security Zone Solution

- Medical devices and their associated systems are grouped together in an internal Security Zone (also referred to as a Community of Interest)
- Provides a layer of security by incorporating implicit access control lists on the OSSR, ISSR, and managed switches
- Provides an additional layer of security by incorporating implicit rulesets on the Firewall
- Adds another layer of security by inserting an IPS sensor inside the Security Zone

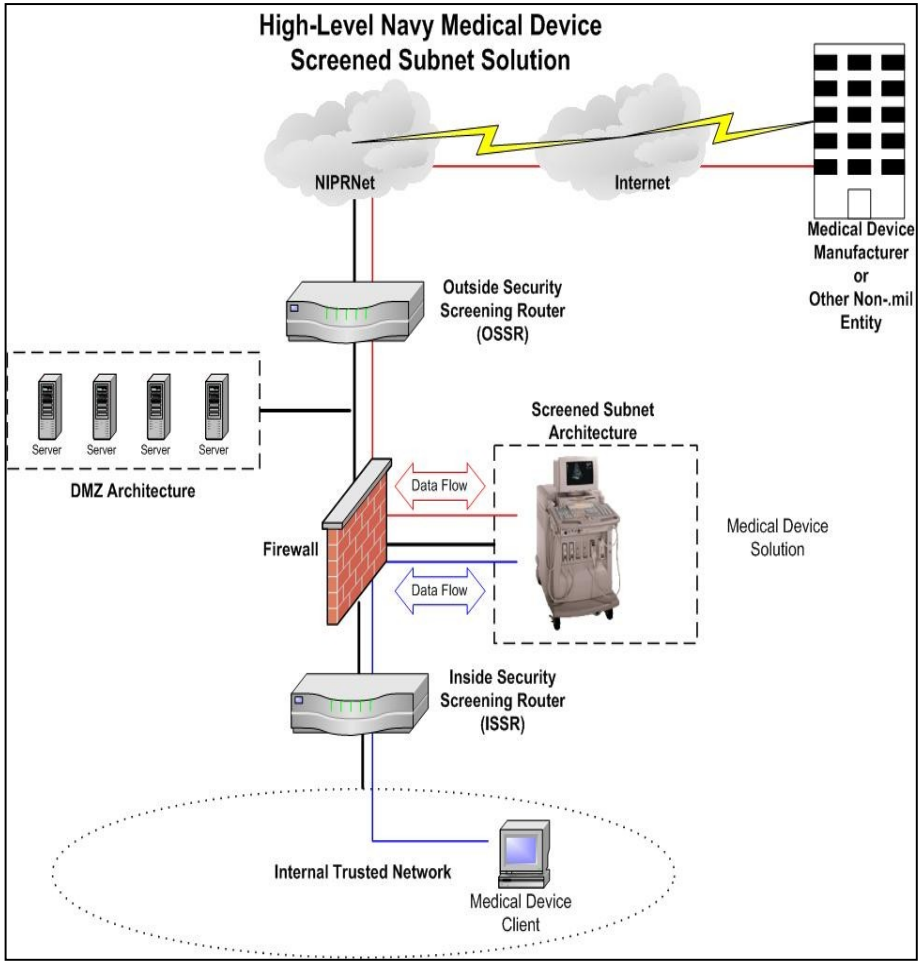


Used within trusted network or when using compliant ports across boundaries

Screened Subnet

Screened Subnet Solution

- Provides more security than a standard DMZ architecture
- Provides a layer of security by incorporating implicit access control lists on the OSSR, ISSR, and managed switches
- Provides another layer of security by incorporating implicit rulesets on the Firewall
- Adds another layer of security by inserting an IPS sensor inside the Security Zone
- Is in compliance with DoD Policy for communications to a non .mil domain



Used to communicate outside trusted network

STIG Current Status

- Medical Device STIG has been signed and in force for just over 6 months
- Sites have had the opportunity to implement it to whatever degree necessary to protect both their networks and their medical devices
- This presentation is designed to stir thought for updates required to the STIG
  - Things that did not work properly
  - Things that could be improved
  - Things that should be addressed

Proposed Revisions

- Can be submitted at any time IAW the STIG however input for the next revision will be accepted for the next 3 months
- No specific submission format required
- All submissions must contain the following:
  - POC information
  - Justification and any reference
- Comments, suggestions, etc., can be sent to:
  - DISA-FSO (fso_spt@disa.mil)
  - Bill Crowe (william.crowe.ctr@med.navy.mil), or
  - Chris Cotton (chris.cotton.ctr@med.navy.mil)

Contact Information

- CDR James Martin
- James.L.Martin@med.navy.mil
- 757-953-0503

- CDR Richard Makarski
- Richard.Makarski@med.navy.mil
- 202-762-0037

Questions